Physical Layer Security Using Scrambled BCH with Adaptive Granular HARQ

Azlan Abd Aziz[1](✉), Mohammed Ahmed Magzoub Albashier[1], Azwan Mahmud[2], Mohamad Yusoff Alias[2], and Nurul Asyiqin Amir Hamzah[1]

[1] Faculty of Engineering and Technology, Multimedia University, Cyberjaya, Malaysia
azlan.abdaziz@mmu.edu.my
[2] Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia

Abstract. A dramatic increase in the number of devices that are connected to the wireless networks has seen many challenging issues. One of them is the security problem. Enhancement in physical layer security has shown promising results to improve these security issues in the existing wireless networks. This paper proposes a transmission technique based on scrambled Bose Chaudhuri Hocquenghem code with feedback to improve the physical layer security in wireless communication system. The security of the transmission system over a wiretap channel is investigated. Scrambling matrix is applied to the code word and a hybrid automatic repeat request (HARQ) protocol is used. In this paper, the security gap is used as a performance metric to measure the difference between the authorized and unauthorized channel. We find that the proposed technique results in smaller security gap compared to the conventional techniques.

Keywords: security gaps · scrambled BCH · Adaptive HARQ

1 Introduction

The rapid growth of wireless communication networks in recent years is the main concern among scientists, researchers and engineers about the security and reliability of the wireless devices [1]. The open nature of the wireless communication networks where the signal propagates in the free space makes it vulnerable to cyber attacks [2]. The existing security of the wireless communication networks is typically implemented in the upper layers of the Open System Interconnection model (OSI) such as, application layer, transport layer and network layer. The existing security is based on the cryptography techniques.

Cryptography is mostly based on secret key that is shared between the transmitter and receiver. The cryptography techniques assume that the unauthorized receivers have a limited computational power [3]. This assumption has not been realistic as super computers and quantum computers are becoming a reality very soon [4]. For all the above reasons, the idea of having security at the physical layer has been proposed. There are many advantages of having the security at the physical layer such as, the channel is responsible of the security which disregards the secret key sharing, all the users have the

M. Y. bin Alias (Ed.): MECON 2022, AER 214, pp. 58–67, 2023.
https://doi.org/10.2991/978-94-6463-082-4_8

full channel state information about the transmission technique and most importantly, the physical layer security doesn't assume a limitation of the computational power of the unintended receiver [5].

2 Related Works

The studies of the wire-tap channel capacity have been investigated in decades and some authors have presented their findings in [2] and [3]. The literature suggests that an increasing interest in the coding techniques applied on the wire-tap channel is encouraging [3, 7]. Here, we focus on the Additive White Gaussian Noise (AWGN) wire-tap model assuming the secrecy capacity equal to the difference between the two channel capacities [8]. For a secure transmission, Bob (receiver) channel is assumed to be higher in the signal-to-noise ratio (SNR) than that in Eve (eavesdropper) channel. This is typically achieved by using feedback channel between Alice (sender) and Bob which Eve has an access as well [9].

To analyze the above situation, an important performance metric is the security gap, which measures the security level by using bit error rate and it was introduced by Klinc in [9]. It is assumed that the SNR received at Bob is higher than the SNR received at Eve. In order for us to achieve physical layer security, the average bit error rate for Eve channel must be at least 0.5 which means half of the message is corrupted and the average bit error rate of Bob channel must get close to 0. The security gap should be as small as possible so that the desired security is achieved with small degradation of Eve channel [9]. Error correcting code like low density parity checks (LDPC) is used to improve the security gap. Nowadays, since the aim is to design physical layer security approaches with small security gap, several methods have been successfully implemented. Most of the implemented algorithms are based on LDPC. The idea of the security gap illustrated in Fig. 1 can be explained in the following expressions.

$$S_g = \left.\frac{\overline{E}_b}{N_0}\right|_B - \left.\frac{\overline{E}_b}{N_0}\right|_E \tag{1}$$

where $\left.\frac{\overline{E}_b}{N_0}\right|_B$ and $\left.\frac{\overline{E}_b}{N_0}\right|_E$ are such that

$$\overline{P}_e^B = f\left(\left.\frac{\overline{E}_b}{N_0}\right|_B\right), \overline{P}_e^E = f\left(\left.\frac{\overline{E}_b}{N_0}\right|_E\right) \tag{2}$$

where S_g is the security gap, $\left.\frac{\overline{E}_b}{N_0}\right|_B$ is the signal to noise ratio of the intended receiver Bob, $\left.\frac{\overline{E}_b}{N_0}\right|_E$ is the signal to noise ratio of the eavesdropper Eve. The bit error rate for Bob is denoted by $\overline{P}_e^B$ while the bit error rate for Eve is denoted by $\overline{P}_e^E$. The security in this content is achieved when the bit error probability of Bob P_e^B is lower than the threshold $\overline{P}_e^B$ while the bit error probability of Eve P_e^E is greater than the Eve threshold PE $\overline{P}_e^E$.

In this paper, unlike in the previous schemes, we propose to improve the security gap by employing a hybrid automatic repeat-request (HARQ) protocol with a scrambling

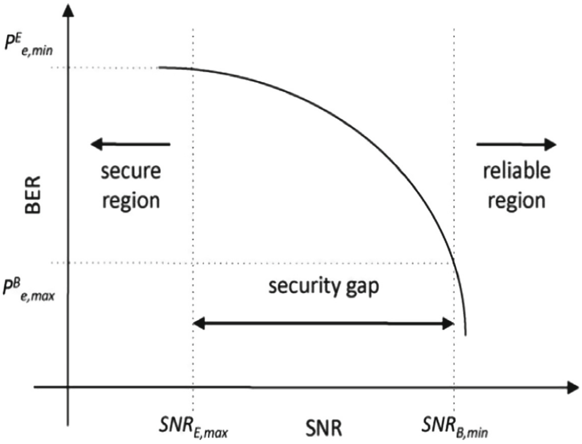

Fig. 1. Security Gap [9]

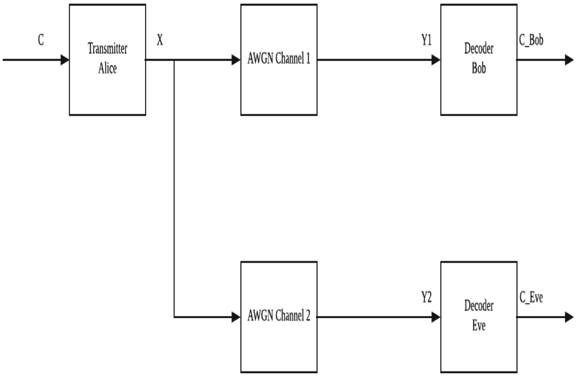

Fig. 2. Wiretap Model [10]

matrix, in which the information bits are made hidden in the transmitted codewords, due to scrambling method and from multiple requests of retransmission from the intended receiver. Specifically, we show that by employing some error correcting codes which are based on punctured codes, non-systematic codes, with a certain set of parameters our proposed schemes result in smaller secrecy gaps and outperform the other conventional schemes. In the case of hard-decoded error correcting codes like block codes (i.e., BCH codes), it can alternatively be an effective option.

The simplest model to represent the physical layer security is the wiretap channel ss shown in Fig. 2. As Wyner showed in [10] that the perfect security can be conducted without sharing secret key only when the legitimate receiver channel (main channel) is better than the eavesdropper channel. The wiretap channel consists of one sender which is Alice and two receivers (see Fig. 2), the legitimate receiver Bob and the eavesdropper Eve [6].

The model indicates that both Bob and Eve receive the transmission from Alice but they are using different channels. The wiretap channel refers to the second channel which is between Alice and Eve (the eavesdropper). The first channel is the main channel between Alice and Bob [7]. Both channels are assumed to be discrete memoryless channels. One of the characteristics of the wiretap channel is that the main channel is independent of the channel of the eavesdropper or the wiretap channel. The second assumption in the wiretap channel is Alice and Bob agree on the encoding and decoding techniques that are used between them. Eve (the eavesdropper) is fully aware of those encoding and decoding techniques. Eve does not suffer from computational power limitation. These properties allow the physical layer security to be a standalone solution for some of the applications that suffer from memory constraints and processing constraints. Alice is encoding the message *M* and then transmitting it. Both Bob and Eve will receive a different version of the message and we define the message received by Bob as *R* and the one received by Eve as *E*. Additive White Gaussian Channel (AWGN) is used in this scheme. AWGN is giving the same impact that the signal goes through in nature. The input signal to the AWGN is assumed to be binary in the case of physical layer security. The output of the AWGN channel will be a noisier version of the input signal [8].

3 Non-systematics Codes with Physical Layer Security

Non-systematic code for physical layer security is another technique used to improve the security gap or the difference between the channel quality of the intended receiver and the eavesdropper [10]. Scrambling matrix is introduced in this technique to encode the message by multiplying the scrambling matrix by the message. It is found that the problem of the security gap can be further improved through non-systematic codes such as scrambling [11]. Scrambling means that within the transmitted code words, the information bits are kept unclear, as a result of scrambling during encoding. This technique has the advantages that can be combined with error correcting codes to get smaller security gap between Bob and Eve. In order to implement the scrambling. Alice must encode the message as follow [7]:

$$C = U.S.G \tag{3}$$

where **G** is the $k \times n$ generator matrix of an (n,k) linear block code in systematic form and S is a non-singular $k \times k$ binary scrambling matrix. In this paper, we consider the case of $k = n$ and **G** to be coincident with a $k \times k$ identity matrix k.

$$u_B = u = c_l \cdot S^{-1} \tag{4}$$

$$u_E = u = e_l \cdot S^{-1} \tag{5}$$

$$P_e = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{6}$$

While the frame error probability is represented mathematically as

$$P_f = 1 - (1 - P_e)^k \tag{7}$$

$$P_e^{PS} = \frac{1}{2}\left\{1 - \left[1 - \frac{1}{2}erfc\left(\sqrt{\frac{E_b}{N_0}}\right)\right]^k\right\} \tag{8}$$

$$P_e^S = \sum\nolimits_{j=0}^{k} P_j \sum_{\substack{i=1\\ iodd}}^{\min(j,w)} P_{i|j} \tag{9}$$

$$P_{i|j} = \frac{\binom{j}{i}\binom{k-j}{w-i}}{\binom{k}{w}} \tag{10}$$

$$P_j = \binom{k}{j} P_e^j (1 - P_e)^{k-j} \tag{11}$$

We assume the intended receiver Bob can detect and correct all the error as Eq. (4). On the other hand, Eve is the unintended receiver who is going to receive the message with an error represented by Eq. (5). In the case of absence of the scrambling metric implemented on the message, the code is considered to be systematic where we calculate the bit and frame error probability as shown in Eq. (6) [12].

The bit error probability after descrambling in the case of perfect scrambling is found to be as half of the frame error probability and it is shown by Eq. (8). We denote it by $w \leq k$ the column weight of matrix S^1, that we assume it to be regular for simplicity. Let P_j be the probability that a received *k-bit* vector contains j errors before descrambling, and $P_{i|j}$ the probability that exactly i out of j errors are selected by a weight w column of S^{-1}. Under such assumptions, the bit error probability on each received bit, after descrambling, can be expressed in Eqs. (9), (10) and (11). In the presence of any error correcting codes such as LDPC, BCH or Reed Solomon the probability P_j that the first k bits (are necessary to be descrambled in order to get the information bits) contains errors that is equal to j can be calculated by Eq. (11) [12].

3.1 Bose-Chaudhuri-Hocquenghem (BCH)

BCH was invented by Raj Bose, D.K.Ray-Chaudhuri, and Alexis Hocquenghem. BCH is one of the error correcting codes that can detect and correct multiple bits error. BCH can be constructed based on Galois field. BCH is one of the error correcting codes that is suitable for wireless sensor networks due to its characteristics of improving the energy efficiency by 23 percent than the uncoded. BCH is chosen to be scrambled codes in order to decrease the security gap between the legitimate receiver and eavesdropper. Through scrambling, BCH has shown some improvement in the security.

4 Granular HARQ with BCH Codes

In granular HARQ, the first transmission $q = 1$ considers a packet with the whole codeword and the subsequent transmissions $q > 1$ considers a subdivision of the codeword into g sub-packets. By neglecting the correlation between tretransmissions, the frame error probability after receiving q packets in a granular HARQ is given by Eq. (12). Setting g to 1 in (16) reduces to Eq. (13). The Probability that exactly $1 \leq Q \leq Q_{max}$ packets are transmitted is given by Eq. (15), while Eq. (14) calculates the frame error probability for Bob and Eve, with G-HARQ protocol.

In previous sections, both scrambling technique and the granular HARQ are discussed independently. In this section scrambling matrix is introduced to the granular HARQ. The security gap of the system depends on two variables, the density of the scrambling matrix as well as the level of the granularity. The effect of the density of the scrambling matrix has been found to be more critical, significant and sensitive to the results than the effect of the granularity. The relationship between the granularity, scrambling matrix density and the security gap is the focus in this subsection. The density of the scrambling matrix is inversely proportional to the security gap as shown in the previous works. The higher the density of the scrambling matrix, the smaller the security gap we willget. In this work, we show that another factor can be added in addition to the density of the sscrambling matrix which is the granularity. Our results show that both granularity and the density of the scrambling matrix result in achieving smaller security gap. It is found that, the higher number we divide the message to when we re transmit the message by the request of the legitimate receiver (granularity), the smaller security gap we can get. The frame error probability after receiving q packets and the granular g is greater than one is expressed by the following mathematical equation.

$$P_q = \frac{1}{2}\operatorname{erfc}\left(\sqrt{q\frac{k}{n}\frac{E_b}{N_0}}\right) \tag{12}$$

$$\mathbf{F}(q) \approx \sum_{e=t+1}^{n} \binom{n}{e} (P_q)^e (1 - P_q)^{n-e} \tag{13}$$

$$\begin{aligned} \mathbf{H}^B &= T(Q_{\max}) \times \mathbf{F}^B(Q_{\max}) \\ \mathbf{H}^E &= \sum_{Q=1}^{Q_{\max}} \left[\mathbf{T}(Q) \cdot \prod_{q=1}^{Q} \mathbf{F}^E(q) \right] \end{aligned} \tag{14}$$

$$\Gamma(Q) = \begin{cases} \prod_{q=1}^{Q-1} \mathbf{F}^B(q) \times \left[1 - \mathbf{F}^B(q)\right] & 1 \leq Q < Q_{\max} \\ \prod_{q=1}^{Q-1} \mathbf{F}^B(q) \times \left[1 - \mathbf{F}^B(q)\right] & 1 \leq Q < Q_{\max} \\ \prod_{a=1}^{Q-1} \mathbf{F}^B(q) & Q = Q_{\max} \end{cases} \tag{15}$$

$$\begin{aligned} \boldsymbol{F}(Q) \approx & \textstyle\sum_{e_1=0}^{n_1 \equiv [(q-1) \div g] \frac{n}{g}} \binom{n_1}{e_1} \left(P_{\left\lceil \frac{q}{g} \right\rceil + 1}\right)^{e_1} \\ & \sum_{e_2=[t+1-e_1]^+}^{n-n_1} \binom{n-n_1}{e_2} \left(P_{\left\lceil \frac{q}{g} \right\rceil}\right)^{e_2} \left(1 - P_{\left\lceil \frac{q}{g} \right\rceil}\right)^{n-n_1-e_2} \end{aligned} \tag{16}$$

Obviously from Eq. (16), we find that when $g = 1$, it reduces back to Eq. (13).

5 Results and Discussions

In this section, the proposed scheme is simulated by using several values of granularities g and column weight w of the scrambling metrics. Table 1 shows the simulation parameters used in Matlab.

Figure 3 shows the signal to noise ratio versus the bit error rate. From the figure, the scrambling is affecting the bit error probability performance, and scrambling is making the bit error probability goes to 0.5. In addition, the security gap is reduced by the scrambling as the slope of the bit error probability improved. The highest error probability is achieved by the perfect scrambling. In addition, the figure shows that the bit error probability is depending on the column weight w of the descrambling matrix S^{-1}. However, the performance of the scrambling matrix with column weight $w = 100$ or $w = 300$ is not far from the perfect scrambling performance. The density of the matrix with $w = 100$ is approximately 0.26, which means that it is not compulsory to reach a 0.5 matrix density in order to get a perfect scrambling. From a complexity point of view the lower the density of the scrambling matrix the less complexity because of the operations needed to perform the descrambling.

Figure 4 shows the simulation results for the security gap versus the bit error rate of the unintended receiver Eve with regard to the scrambling metric in addition to the HARQ

Table 1. Simulation Parameters

n	510
k	384
g	2,3,10
C	3
q	$=((C - 1) * g) + 1;$
SNR_g	0:0.5:27
w	5, 20, 100, 300

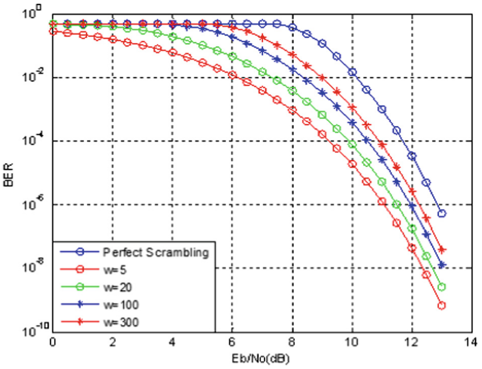

Fig. 3. Scrambling Levels

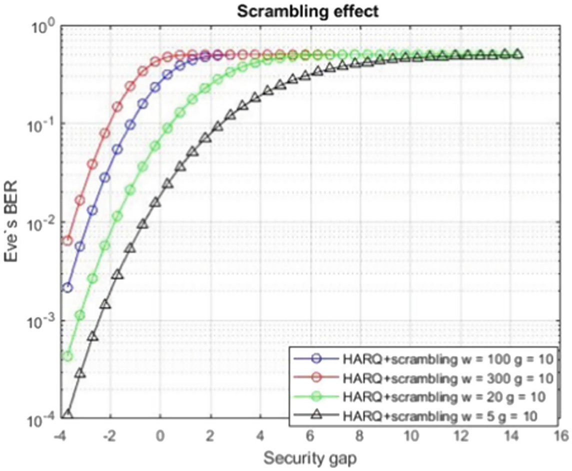

Fig. 4. Different scrambling metrics intensity w

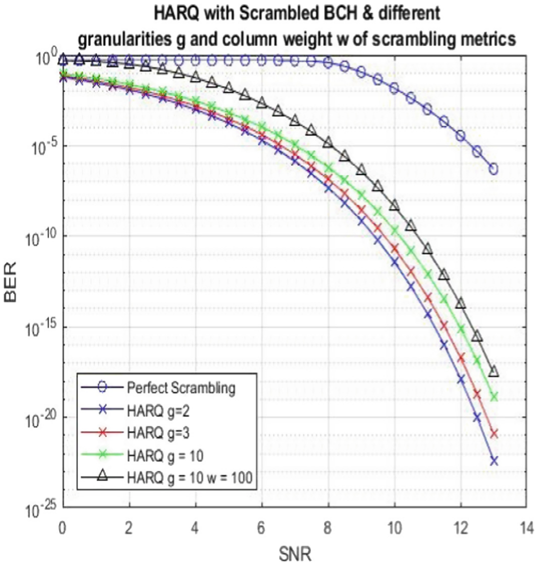

Fig. 5. HARQ with granularity $g > 1$

protocol with fixed granularity. The effect of the intensity of the scrambling metrics has been evaluated. The higher the intensity of the scrambling metric the smaller security gap we achieve.

Figure 5 shows the effect of the different granularity applied with the comparison to the perfect scrambling. When the granularity is high with high intensity of the scrambling metrics the results is very close to the perfect scrambling at small security gap. Figure 6 is showing the effect of different granularity with fixed scrambling metrics $w = 10$ which

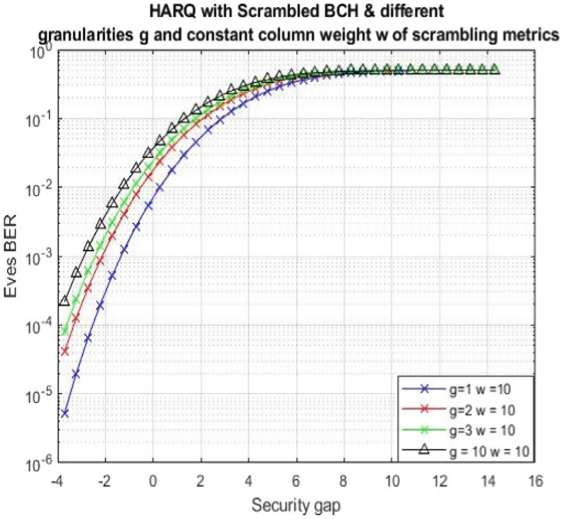

Fig. 6. HARQ with granularity $g > 1$

consider low intensity. The effect of the granularity can be significant depending on the intensity of the scrambling metric.

6 Conclusion

Our proposed scheme has shown that a significant improvement in the security gap can be achieved by using scrambled BCH with granularity. The simulation results show that security gap is directly proportional to the granularity and the scrambling matrix density. The higher the density of the matrix and the granularity the smaller security gap can be obtained and hence, the security of the system can further be improved.

Acknowledgment. We would like to acknowledge Telkom University for providing financial sponsorship to facilitate this research project under Telkom-MMU Research Grant 2021 (Project Code: MMUE/210067).

References

1. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends, “*Proceedings of IEEE*, vol. 104, p. 1727 1765, Sep.2016
2. U. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inform. Theory, vol. 39, no. 3, pp. 733–742, May 1993.
3. G. Shamir, J. Boutros, A. Alloum, and L. Wang, “Non-systematic LDPC codes for redundant data,” *in Proc. Inaugural Workshop for the Center of Information Theory and its Applications*, San Diego, California, Feb. 2006.
4. W. Harrison and S. McLaughlin, “Physical-layer security: Combining error control coding and cryptography,” *in Proc. IEEE International Conference on Communications (ICC ‘09)*, Dresden, Germany, Jun. 2009, pp. 1–5.

5. D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, “LDPC codes for physical layer security,” *in Proc. IEEE Global Telecommunications Conference (GLOBECOM 2009)*, Honolulu, HI, Nov. 2009, pp. 1–6.
6. M. Bloch and J. Barros, Physical Layer Security From Information Theory to Security Engineering. *Cambridge University Press*, 2011.
7. M. Baldi, M. Bianchi, and F. Chiaraluce, “Coding with Scrambling, Concatenation and HARQ for AWGN Wire-Tap Channel: A Security Gap Analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883-894, June 2012.
8. A. Amirzadeh , M. Haj Taieb and J-Y. Chouinard, “Physical Layer Secrecy for Wireless Communication Systems using Adaptive HARQ with Error Contamination,” *2017 15th Canadian Workshop on Information Theory (CWIT)*, June 2017, Quebec, Canada.
9. M. Haj Taieb and J-Y. Chouinard, “Reliable and Secure Communications over Gaussian Wiretap Channel Using HARQ LDPC Codes and Error Contamination,” *2nd Workshop on Physical layer Methods for Wireless Security*, pp. 669–674, September 2015, Florence, Italy.
10. Alireza Nooraiepour, Sina Rezaei Aghdam, Tolga M. Duman, “On Secure Communications Over Gaussian Wiretap Channels via Finite-Length Codes,” *IEEE Commun. Lett*. 24(9): 1904–1908, 2020.
11. Zhang, N. Jiang, S. Liu, A. Zhao, J. Peng, and K. Qiu, “Physical Layer Security Encryption in CO-OFDM based on Chaotic 3D Constellation Scrambling,” *Asia Communications and Photonics Conference 2021*, T4A.112.
12. C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, April 1949.